Cyberoam CR1000iNG-XP UTM Firewall

Product Name: Cyberoam CR1000iNG-XP UTM Firewall
Manufacturer: Cyberoam
Model Number: CR1000iNG-XP

Cyberoam CR1000iNG-XP UTM Firewall
The Cyberoam CR1000iNG-XP UTM Firewall offers inline application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN (IPSec and SSL) and granular bandwidth controls. Additional security features like WAF, Gateway AntiVirus, Anti-Spam are also available. The FleXi Ports (XP) available in CR1000iNG-XP appliances offer flexible network connectivity with I/O slots that allow additional Copper 1G, Fiber 1G/10G ports on the same security appliance.
Cyberoam CR1000iNG-XP Key Features

• Maximum number of Available Ports 42
• Fixed Copper GbE Ports 10
• Number of Slots for FleXi Ports Module* 4
• Port Options for FleXi Ports Module (GbE Copper / GbE Fiber / 10GbE Fiber) 8,4 / 8 / 4
• Console Ports (RJ45) 1
• USB Ports 2
• Configurable Internal/DMZ/WAN Ports Yes

Cyberoam CR1000iNG-XP - Technical Specifications

System Performance**

• Firewall Throughput (UDP) (Mbps) 120,000
• Firewall Throughput (TCP) (Mbps) 45,000
• New sessions/second 240,000
• Concurrent sessions1 3,000,000
• IPSec VPN Throughput (Mbps) 5,000
• No. of IPSecTunnels 8,000
• SSL VPN Throughput (Mbps) 850
• WAF Protected Throughput (Mbps) 2,000
• Anti-Virus Throughput (Mbps) 8,000
• IPS Throughput (Mbps)12,500
• NGFW Throughput (Mbps)*** 7,250
• Fully Protected Throughput (Mbps)**** 5,800

Stateful Inspection Firewall

• Layer 8 (User Identity) Firewall
• Multiple Security Zones
• Location-aware and Device-aware Identity-based Access Control Policy
• Access Control Criteria (ACC): User-Identity, Source and Destination Zone, MAC and IP address, Service
• Security policies IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and QoS
• Country-based Traffic Control
• Access Scheduling
• Policy based Source and Destination NAT, Gateway Specific NAT Policy
• H.323, SIP NAT Traversal
• DoS and DDoS attack prevention
• MAC and IP-MAC filtering
• Spoof Prevention

Intrusion Prevention System

• Signatures: Default (4500+), Custom
• IPS Policies: Pre-configured Zone-based multiple policies, Custom
• Filter based selection: Category, Severity, Platform and Target (Client/Server)
• IPS actions: Recommended, Allow Packet, Drop Packet, Disable, Drop Session, Reset, Bypass Session
• User-based policy creation
• Automatic signature updates via Cyberoam Threat Research Labs
• Protocol Anomaly Detection
• SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

Application Filtering

• Layer 7 (Applications) & Layer 8 (User Identity) Control and Visibility
• Inbuilt Application Category Database
• Control over 2,000+ Applications classified in 21 Categories
• Filter based selection: Category, Risk Level, Characteristics and Technology
• Schedule-based access control
• Visibility and Controls for HTTPS based Micro-Apps like Facebook chat, Youtube video upload
• Securing SCADA Networks
• SCADA/ICS Signature-based Filtering for Protocols Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
• Control various Commands and Functions

Administration & System Management

• Web-based configuration wizard
• Role-based Access control
• Support of API
• Firmware Upgrades via Web UI
• Web 2.0 compliant UI (HTTPS)
• Command Line Interface (Serial, SSH, Telnet)
• SNMP (v1, v2, v3)
• Multi-lingual : English, Chinese, Hindi, French, Japanese
• Cyberoam Central Console (Optional)

User Authentication

• Internal database
• AD Integration and OU-based Security Policies
• Automatic Windows/RADIUS Single Sign On
• External LDAP/LDAPS/RADIUS database Integration
• Thin Client support
• 2-factor authentication: 3rd party support*****
• SMS (Text-based) Authentication Layer 8 Identity over IPv6
• Secure Authentication – AD, LDAP, Radius
• Clientless Users
• Authentication using Captive Portal

* Additional purchase required. FleXi Ports are not HOT swappable.Appliance needs to be turned off prior to changing the FleXi Ports Modules. ** Antivirus, IPS and Fully Protected Throughput performance is measured based on HTTP traffic as per RFC 3511 guidelines. Actual performance may vary depending on the real network traffic environments. *** NGFW throughput is measured with Firewall, IPS and Web & Application Filtering features turned on.

Please Enquire